UNITED STATES DISTRICT COURT FOR
THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

COMMUNICATION TECHNOLOGIES, INC. Plaintiff, v. SAMSUNG ELECTRONICS AMERICA, INC. and SAMSUNG ELECTRONICS CO., LTD., Defendants.	CIVIL ACTION NO. 2:21-cv-00444-JRG JURY TRIAL DEMANDED

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Communication Technologies, Inc. ("COMTek" or "Plaintiff") hereby sets forth its Second Amended Complaint for Patent Infringement against Defendants Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. ("Samsung" or "Defendants"), and states as follows:

NATURE OF THE CASE

1. This action is for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, et seq. COMTek seeks monetary damages and injunctive relief in this action.

THE PARTIES

2. Plaintiff COMTek is a corporation organized and existing under the laws of the State of Virginia, having its principal office at 11710 Plaza America Drive, Suite 2000, Reston, Virginia 20190.

3. COMTek is a leading technology firm which offers an array of telecommunications and IT managed services as well as training support to government and commercial enterprises. In 2001, the Department of Defense recommended COMTek's patented solution in the form of COMTek's No*Trace software application. Notably, COMTek's software was listed first among the five products that the DoD considered to meet its minimum policy standards.

4. Upon information and belief, Defendant Samsung Electronics America, Inc. is a New York corporation with a principal place of business at 6625 Excellence Way, Plano, TX 75023, and a subsidiary of Samsung Electronics Co., Ltd. Headquartered in Suwon, South Korea.

5. Upon information and belief, Defendant Samsung Electronics Co., Ltd. Is a corporation organized and existing under the laws of the Republic of Korea with a principal place of business at 129, Samsung-ro, Yeongstong-gu, Suwon-si, Gyeonggi-Do, Lorea 443-742.

JURISDICTION AND VENUE

6. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

7. This Court has personal jurisdiction over Defendants on the grounds that Samsung has minimum contacts with the State of Texas and has purposefully availed itself of the privileges of conducting business in Texas including through, at least, setting up an office in Texas as well selling and offering for sale of products accused of infringement in this action throughout Texas.

8. Venue is proper in this district pursuant to 28 U.S.C. § 1400(b) because Samsung has engaged in acts of infringement in this district and has a regular and established place of business in this district.

FACTUAL BACKGROUND: COMTEK AND THE PATENTED TECHNOLOGY

COMTek's Origins

9. Plaintiff COMTek was established in October 1990 by Dr. Joseph Fergus, a former AT&T Bell Laboratories ("Bell Labs") engineer and Vietnam-era veteran of the U.S. Navy.[1] Dr. Fergus started the company after spending approximately 10 years at Bell Labs, widely regarded as the most prestigious Research and Development (R&D) organization in information and communication technology (ICT) at the time. During his tenure at Bell Labs, Dr. Fergus worked on a number of technological innovations including, Signaling Systems No. 7 (SS7) for telecommunications network, the Integrated Services Digital Networks (ISDN), the Signaling Network Interconnection (SNI) gateway function and Open Systems Interconnection (OSI) standards. In addition, Dr. Fergus was a United States Representative to the Consultative Committee for Telephony and Telegraphy (CCITT) (now called the International Telecommunications Union – Telecommunication Standardization Sector (ITU-T)) in Geneva, Switzerland, where he helped to advance US positions on international telecommunication standards development. Among his accomplishments are: 1) the development of the Seize Circuit Procedure, which was responsible for call set-up between in-band and out-of-band

[1] Dr. Fergus is from the Island of St. Croix in the U.S. Virgin Islands. He received his Doctorate of Humane Letters from Norfolk State University in 2004. He holds a Masters Degree from the University of Illinois and a Bachelors Degree in Electrical Engineering from Norfolk State University. He has been the recipient of several awards including the "Minority Business Leader" Award (Washington Business Journal), "Excellence in Leadership" Award (Northern Virginia Urban League), "Best of Black Business" Award (American Academy of Business and Commerce), and the Top Black Business Award (DiversityBusiness.com).

signaling networks; 2) the creation of the Charge Number Parameter, which enables the transport of caller identification (Caller ID) information across multiple signaling networks; and 3) significant contribution towards the development of the Signaling Connection Control Part (SCCP) – a network/session layer function of the signaling network protocol stack that allows for virtual call establishment. It was this deep understanding of and multifaceted expertise in telecommunications, along with the desire to establish his own enterprise that drove Dr. Fergus toward the creation of COMTek.

10. During the 1990s, COMTek provided systems engineering and technical assistance to the federal government of the United States as well as the private sector. Because of Dr. Fergus's background and expertise, COMTek was contracted to provide technology research to the Department of Defense ("DoD") including producing technical reports on such topics as 1) the transition from Internet Protocol Version 4 (Ipv4) to Internet Protocol Version 6 (Ipv6); 2) the effects of electromagnetic pulse on electronic systems; and 3) the standardization of Multi-Level Precedence and Pre-emption (MLPP) application, to name a few. COMTek also provided other ICT standards development support as well as other technical expertise to include computer facilities management (*i.e.,* 24/7 enterprise systems operations and technical support, including systems programming, application programming and systems maintenance), systems break/fix support and data custodian support. Data custodian was the term used by the DoD to describe the support for end-of-life computer systems.

11. During this same period, the DoD was concerned that data resident on storage media in end-of-life systems could fall into the wrong hands. Therefore, COMTek was tasked by the United States Air Force (USAF) with collecting end-of-life systems, removing the hard drives, degaussing the hard drives, and having them shredded by an industrial shredder. After

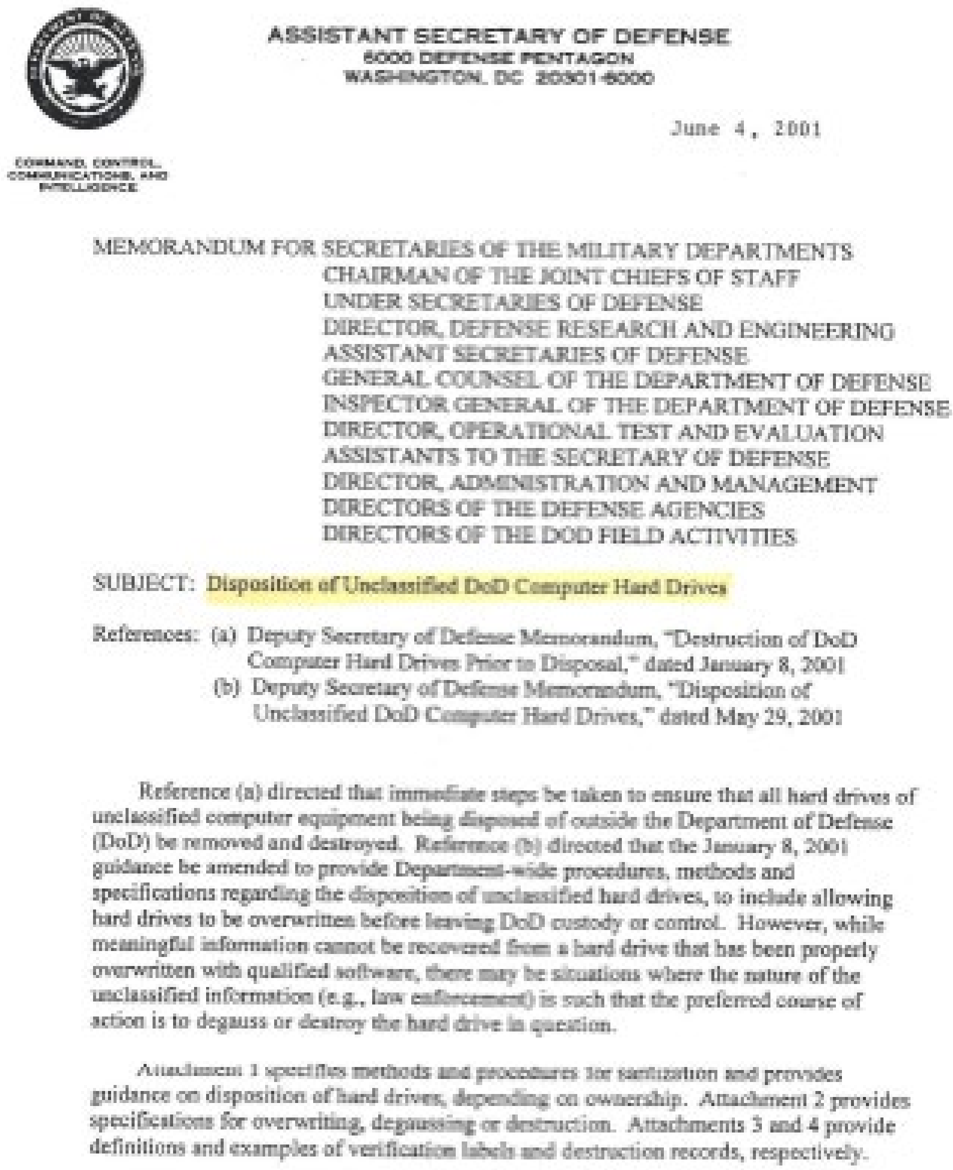
processing several thousand systems and shredding their drives, and realizing the onerous time required to physically shred hardware, COMTek created a software solution that eliminated the need to remove the hard drives, and thereby automating the data removal process. As new Pentium computers were rapidly introduced into the marketplace, so too were older systems being placed into the end-of-life category. The conventional thinking at the time was that any, or all, of the end-of-life devices could have sensitive information stored on them and, therefore, such data must be protected.

*No*Trace and the Patented Technology*

12. COMTek also learned through its marketing efforts to the U.S. Army Communication and Electronics Command (CECOM) at Fort Monmouth, New Jersey that the DoD was considering issuing laptop computers to U.S. troops. However, the DoD was concerned that such devices could fall into the wrong hands and a solution was needed. When Dr. Fergus learned of the dilemma, he invented a solution, claimed in what would become U.S. Patent No. 6,725,444 ("the '444 patent"), and commercialized it in COMTek's "No*Trace" application. The No*Trace application provided the DoD with a way to protect sensitive data resident on mobile devices, even when such devices were not in the possession of their rightful owners.

13. Dr. Fergus's system and method for handling and protecting sensitive data on mobile computing devices was groundbreaking. When the DoD learned that, using Dr. Fergus's system and method, data could be permanently removed from (and thereby protected on) mobile computing devices without removing the storage medium (*e.g.*, hard drive) and, that overwriting could be done without limits to the number of times the data can be overwritten, the DoD

released guidelines on the handling of sensitive data on mobile devices, titled "Disposition of Unclassified DoD Computer Hard Drives."



ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

June 4, 2001

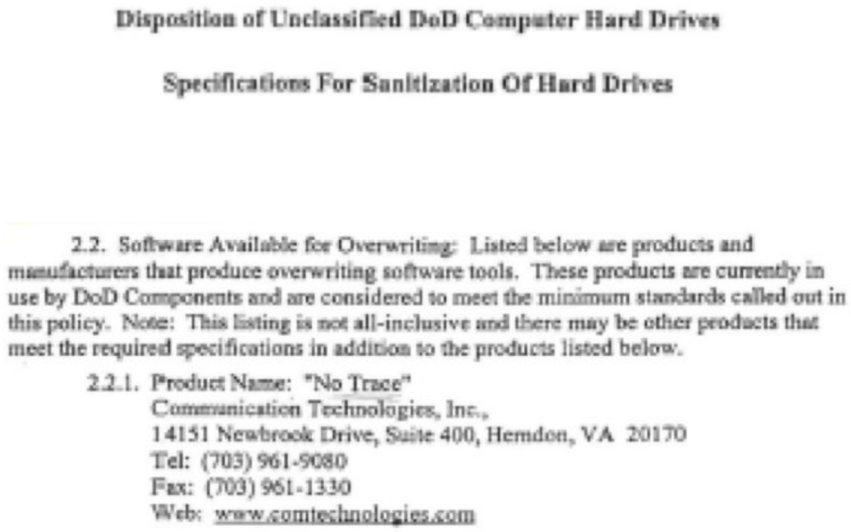
MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Disposition of Unclassified DoD Computer Hard Drives

References: (a) Deputy Secretary of Defense Memorandum, "Destruction of DoD Computer Hard Drives Prior to Disposal," dated January 8, 2001
(b) Deputy Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated May 29, 2001

Reference (a) directed that immediate steps be taken to ensure that all hard drives of unclassified computer equipment being disposed of outside the Department of Defense (DoD) be removed and destroyed. Reference (b) directed that the January 8, 2001 guidance be amended to provide Department-wide procedures, methods and specifications regarding the disposition of unclassified hard drives, to include allowing hard drives to be overwritten before leaving DoD custody or control. However, while meaningful information cannot be recovered from a hard drive that has been properly overwritten with qualified software, there may be situations where the nature of the unclassified information (e.g., law enforcement) is such that the preferred course of action is to degauss or destroy the hard drive in question.

Attachment 1 specifies methods and procedures for sanitization and provides guidance on disposition of hard drives, depending on ownership. Attachment 2 provides specifications for overwriting, degaussing or destruction. Attachments 3 and 4 provide definitions and examples of verification labels and destruction records, respectively.



Disposition of Unclassified DoD Computer Hard Drives

Specifications For Sanitization Of Hard Drives

2.2. Software Available for Overwriting: Listed below are products and manufacturers that produce overwriting software tools. These products are currently in use by DoD Components and are considered to meet the minimum standards called out in this policy. Note: This listing is not all-inclusive and there may be other products that meet the required specifications in addition to the products listed below.

2.2.1. Product Name: "No Trace"
Communication Technologies, Inc.,
14151 Newbrook Drive, Suite 400, Herndon, VA 20170
Tel: (703) 961-9080
Fax: (703) 961-1330
Web: www.comtechnologies.com

Awards and Recognition

15. In 2004, Fergus's leadership was recognized nationally when COMTek earned a spot on the prestigious "Inc. 500" list of the fastest-growing private companies in America. COMTek was also listed as one of the top 100 Black-owned businesses in the United States, ranking in the top one percent of all minority-owned business in the country.

16. In 2009, the Washington Business Journal published an article entitled "Joseph Fergus: Digital eraser" which described a consumer-focused version of the patented technology. *See* https://www.bizjournals.com/washington/stories/2009/11/09/story8.html?s=print.

THE PATENT-IN-SUIT

17. This case involves U.S. Patent No. 6,725,444 ("the '444 Patent" or "the Asserted Patent"). A copy of the '444 Patent is attached as Exhibit A.

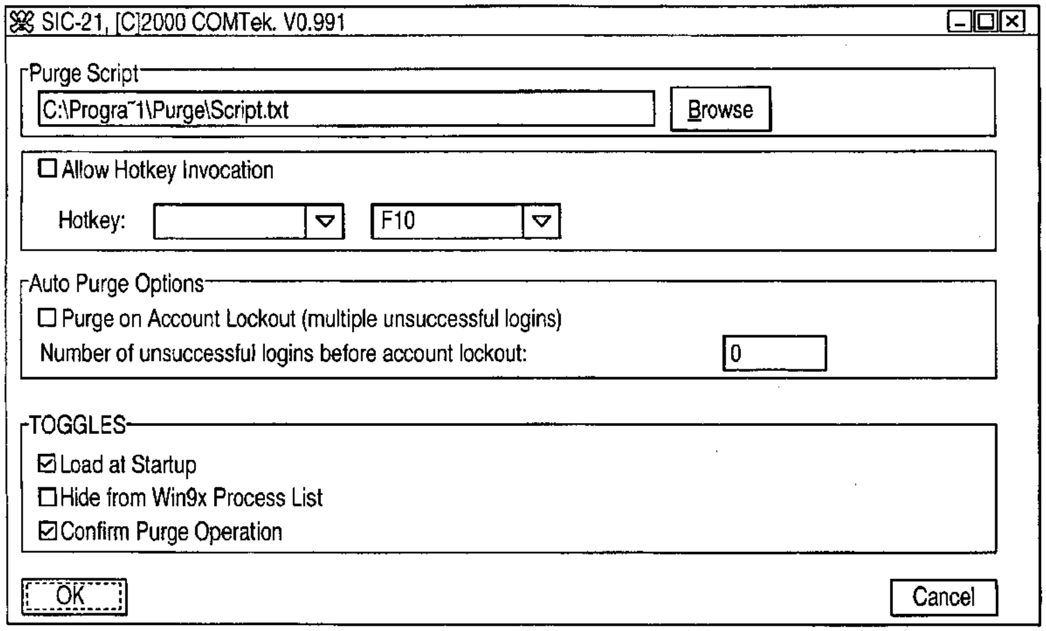
18. As explained in the '444 Patent, computing systems may "contain sensitive information related to a corporation or entity's business, personnel, finances, or technology." (Ex. A at 1:14-17). "A problem arises when a hostile entity gains access to the computer system and, therefore, possibly access to sensitive information." (*Id.* at 1:21-23). The patent goes on to

describe the "need for systems and methods for removal of sensitive information from computing systems that allows programmability, immediate initiative of removal, automatic initiation of removal of information, as well as bypass protection against hostile entities attempting to circumvent the sensitive information removal process."

19. The '444 Patent is directed to a system and method for programmable removal of information from a computing system that includes: selecting one or more information removal options, where the selecting is performed on a computing device; generating a purge script file based on the selected information removal options; and initiating a purge of information from one or more computing systems, where the purge is performed by execution of the purge script file. *See*, *e.g.*, *Id*. 1:56-63; 2:32:44.

20. Fig. 6 of the '444 Patent shows an example display screen that allows a user to enter options desired during a purge of information. One option is activation of a box "which enables an automatic purge of information to occur upon a particular number of unsuccessful logins." *Id*. 7:49-52.

FIG. 6



SIC-21, [C]2000 COMTek. V0.991

Purge Script

C:\Progra~1\Purge\Script.txt

☐ Allow Hotkey Invocation

Hotkey: F10

Auto Purge Options

☐ Purge on Account Lockout (multiple unsuccessful logins)

Number of unsuccessful logins before account lockout: 0

TOGGLES

☑ Load at Startup

☐ Hide from Win9x Process List

☑ Confirm Purge Operation

21. The ’444 Patent describes that “in systems and methods according to the present invention, the system may be set up to detect a programmable number of unsuccessful logon attempts to a computing system which will thereby initiate automatically the purge of sensitive information from the computing system.” *Id.* at 4:10-15.

22. The ’444 Patent was duly and lawfully issued by the United States Patent and Trademark Office (“USPTO”) on April 20, 2004.

23. The ’444 Patent is assigned to COMTek, which owns all right, title, and interest in the’444 Patent, including the right to sue for infringement and recover damages resulting therefrom.

THE ACCUSED PRODUCTS

24. Defendants offer for sale, sells, and uses within the United States mobile devices including its Galaxy line of phones and tablets, and Tizen products, that utilize Samsung’s Knox mobile security solution and/or Knox Tizen Wearable operating system (Wear OS), to provide a

secure environment for data and apps on Samsung Galaxy and Tizen devices, which solution infringes the '444 Patent. *See*, e.g.,

> https://docs.samsungknox.com/devref/knox-sdk/reference/com/10amsung/android/knox/devicesecurity/PasswordPolicy.html
>
> 10amsung excludeExternalStorageForFailedPasswordsWipe(10amsung enable)
>
> API to include or exclude external storage when device is wiped due to exceeding maximum number of failed password attempts.
>
> 10amsung isExternalStorageForFailedPasswordsWipeExcluded()
>
> API to check whether the external storage is included when device is wiped due to exceeding maximum number of failed password attempts.
>
> https://docs.samsungknox.com/devref/knox-tizen-sdk/group__mdm__password.html,
>
> https://docs.samsungknox.com/devref/knox-tizen-sdk/group__mdm__password.html#ga57842bba93a861ad7731f3517c1264fb
>
> Privilege: http://developer.samsung.com/tizen/privilege/mdm.password
>
> Parameters [in] value The number of failed password attempts, before the device will wipe its data.

Samsung's Knox solutions secure data and apps on a range of devices, providing functionality to erase (or "wipe") data after a set number of unsuccessful attempts entering a passcode or password. Knox's ability to provide data protection to Samsung devices hinges on the systems and methods covered by the '444 Patent.

25. Samsung's Knox solutions offer the capability to partially or completely wipe a device on which it is installed clean, and thereby ensure data doesn't fall into the wrong hands if the device is lost or stolen. *See*, e.g.,

https://www.stigviewer.com/stig/samsung_android_with_knox_1.x/2014-04-22/finding/V-48297. These device wipes may be triggered by entering the wrong passcode, *i.e.*, tied to a selected number of unsuccessful attempts, according to the systems and methods in at least claims 1, 11, and 16.

26. Knox includes security policies that implement device wipes. *See*, e.g., *Id.* and

https://docs.samsungknox.com/devref/knox-sdk/reference/com/samsung/android/knox/devicesecurity/PasswordPolicy.html;

https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11160 (Android 11);

https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11042 (Android 10);

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_SS_Android_OS_9_Knox_3-x_Y20M07_STIG.zip (Android 9); and

https://docs.samsungknox.com/knox-security-technical-implementation-api-guides/knox-3-x-android-9.html#mapping (Android 8)

wherein the wipe can be "complete" in which all of the user space data and user-installed apps are wiped from the device, including any memory cards

(https://docs.samsungknox.com/devref/knox-sdk/reference/com/11amsung/android/knox/devicesecurity/PasswordPolicy.html#excludeExternalStorageForFailedPasswordsWipe(11amsung)); or the wipe can be "selective" in which a Knox container or in which allows "wiping data for a particular application only". *See*, e.g.,

https://docs.samsungknox.com/devref/knox-sdk/reference/com/11amsung/android/knox/container/BasePasswordPolicy.html (public void setMaximumFailedPasswordsForWipe); and

https://developer.android.com/reference/android/app/admin/DeviceAdminReceiver#onPa sswordFailed(android.content.Context,%20android.content.Intent,%20android.os.UserHandle). Wipes may be triggered by entering the wrong passcode, *i.e.*, tied to a selected number of unsuccessful attempts, according to the systems and methods in at least claims 1, 11, and 16.

27. Samsung's KNOX solution's passcode policy allows administrators to customize the threshold for triggering a device wipe or a selective wipe using the field Maximum number of failed passcode attempts to select the maximum number of failed password attempts allowed until all or a portion of the data in the device is wiped. *See*, e.g., *Id*. and

https://www.manageengine.com/mobile-device-management/help/security_management/mdm_security_management.html;

https://developer.android.com/reference/android/app/admin/DeviceAdminReceiver#onPasswordFailed(android.content.Context,%20android.content.Intent); and

https://docs.samsungknox.com/devref/knox-sdk/reference/com/12amsung/android/knox/container/BasePasswordPolicy.html.

The wiping of information tied to a particular number of unsuccessful attempts can therefore be selected according to the systems and methods in at least claims 1, 11, and 16. On information and belief, the selective wipe is accomplished by generating an executable purge script file, based on the selected information removal option.

28. If a user reaches the defined number of failed attempts such that the device is wiped by Samsung's Knox solution, then the device is unavoidably factory reset, or a Knox container is made inaccessible. https://www.samsung.com/za/support/mobile-devices/i-have-forgotten-my-password-for-the-knox-container-what-should-i-do/ The device is then under the direct control of Samsung and cannot be controlled by its user. On information and belief, the factory reset initiates a purge of information automatically by execution of a purge script file

automatically, *i.e.*, setting command(s) for later execution in a memory location, and upon execution of the command(s), erasing of all data after a set number of unsuccessful attempts by overwriting memory locations containing files. Further, on information and belief, the purge comprises deleting file and directory information in a file allocation table or equivalent (e.g. FAT32/exFAT/ext4/F2FS for Android, *see* https://www.samsung.com/ph/support/mobile-devices/how-to-install-the-memory-card-in-samsung-mobile-device/;

https://www.sammobile.com/news/galaxy-note-10-uses-f2fs-not-ext4-file-system-whats-the-difference/) related to the information and overwriting the information in physical memory at least once, wherein sensitive information may be removed from at least one computing device automatically. In order to maintain filesystem consistency, the file allocation table entries are removed as the file data to which they refer is erased.

CLAIM 1
(Infringement of the ’444 Patent by Samsung)

29. Plaintiffs repeat and reallege all preceding paragraphs, as if fully set forth herein.

30. Defendants directly infringe at least claims 1-2, 5-8, 11, 16-17, and 20 of the ’444 Patent in violation of 35 U.S.C. § 271(a) with respect to Defendants’ hardware devices and software applications including, but not limited to its Knox solution as implemented on its Samsung wearable, mobile and other electronic devices. COMTek contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

31. For example, Defendants directly infringe the ’444 Patent by making, using, selling, and/or offering to sell within the United States software applications including, but not limited to, its Knox solution and devices incorporating the Knox solution.

32. COMTek has been injured and seeks damages to adequately compensate it for Defendants' infringement of the '444 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

DAMAGES

33. For the above-described infringement, COMTek has suffered injury and seeks a permanent injunction and damages, in an amount to be proven at trial, to adequately compensate it for Defendants' infringement of the Asserted Patent. Such damages should be no less than the amount of a reasonable royalty under 35 U.S.C. § 284.

JURY DEMAND

34. COMTek requests a jury trial of all issues triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. A judgment in favor of COMTek that Defendants have infringed the '444 Patent, whether literally or under the doctrine of equivalents, as described herein;

B. A judgment and order requiring Defendants to pay COMTek's damages, costs, expenses, and pre-judgment and post-judgment interest for Defendants' infringement of the '444 Patent and provided under 35 U.S.C § 284, including supplemental damages for any continuing post-verdict or post-judgment infringement with an accounting as needed; and

C. A judgment and order requiring Defendants to pay COMTek's attorney's fees, costs and disbursements.

D. Such further and additional relief as to the Court deems just and appropriate.

Date: March 14, 2022

By: */s/ Jean-Marc Zimmerman*

Jean-Marc Zimmerman
NJ Bar No. 037451989
Zimmerman Law Group
153 Central Avenue
Westfield, NJ 07090
Telephone: 908-768-6408
Email: jmz@zimllp.com

Steven M. Hoffberg
CT State Bar No. 400760
NY State Bar No. 2353225
Hoffberg & Associates
29 Buckout Road
West Harrison, NY 10604
Telephone: 914-949-2300
Email: steve@hoffberglaw.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: 903-845-5770
Email: ederieux@capshawlaw.com

Attorneys for Plaintiff